Red Teaming and the Hypothesizer Concept

In many ways, the process of intelligence analysis is much like building a puzzle in which many of the pieces are missing and in which the pieces that *are* present are hidden amongst pieces to many other puzzles. The tasks then for the analyst are to first identify when a piece being inspected is significant, to then find other available pieces belonging to the same puzzle, to try to put these pieces into their proper place in the puzzle, and to then try to understand the full picture that the puzzle presents—either by hunting elsewhere for additional pieces or by imagining what the missing pieces might look like. To add this problem, intelligence analysis is almost always a time-sensitive activity. Not only must the puzzle be built, but this must be done quickly enough to allow an adequate response to whatever threat the puzzle indicates.

An idea being explored by Sandia’s Advanced Concepts Group to help address these issues is the use of a “Hypothesizer” (Figure 1). Operating as an adjunct to existing mechanisms for browsing and searching intelligence databases, the Hypothesizer allows an analyst to explore the possible implications of one or more pieces of data (i.e., to hypothesize what kinds of operational scenarios the data might imply) and to then determine what other pieces of data might be found if these operational scenarios were being played out in specific settings by certain actors.

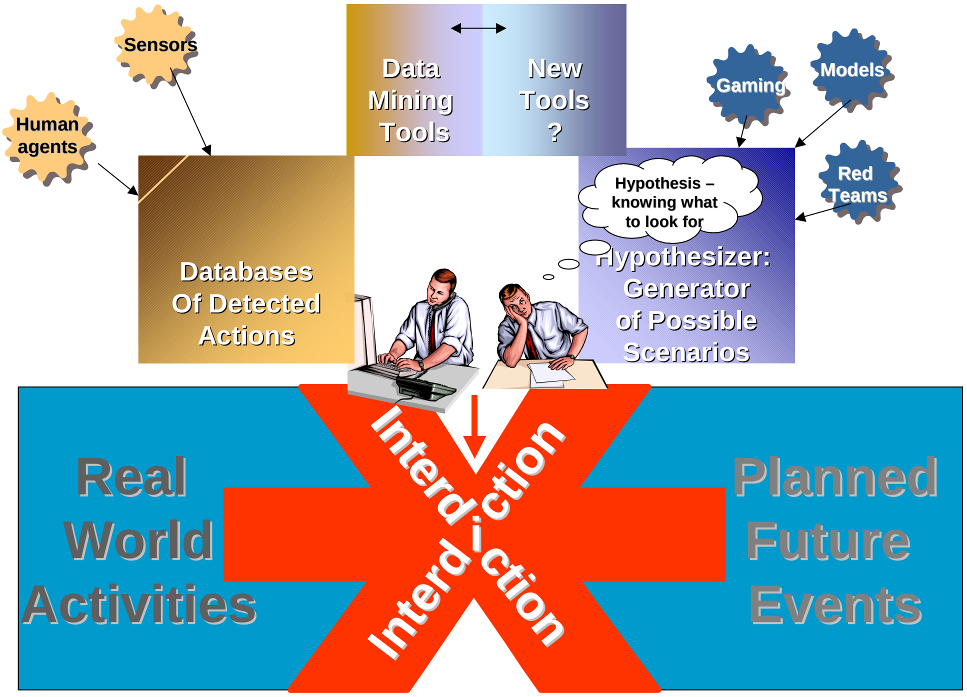

Figure 1. The intersection of analysis with real world data and the hypothetical world of the “hypothesizer” leading to successful interdiction.

In order to support these activities, the Hypothesizer requires a knowledge base of operational methods that can be employed in various scenarios and a means of composing the methods into plans that satisfy analyst-specified criteria. A key question then is how to generate the information required for this knowledge base. The approach being explored by Sandia is the use of Red Teams to generate specific hypothetical scenarios that can then be distilled into their component parts to deliver the desired operational methods. These operational details would be stored in a data warehouse in a format that lends itself of computer manipulation.

Within the national security community, efforts to explore possible terrorist scenarios occur on a regular basis. The hypotheses developed in those events tend to be locally kept, thereby limiting their usefulness to intelligence analysis. The hypothesizer would serve as the repository for the results of these events. In addition, this effort is exploring what would be required to create a national "red gaming" capability to engage in the generation and collection of hypothetical scenarios from a broad range of experts drawn from a diverse set of knowledge domains and to make the knowledge aggregated from this process available to analysts throughout the intelligence community via the proposed Hypothesizer. This process would utilize existing work on red teaming and vulnerability studies, but would add one or more standing Red Team operations working in a gaming environment to develop potential terrorist scenarios. The Red Teaming process would consist of:

- drawing together appropriate red team members for the planned effort,
- using this team to generate the base ideas and operational plans,
- capturing and parameterizing this data,
- perturbing the data to generate still more scenarios, and filtering these by validating their plausibility.

Successfully representing an adversary requires not only that the team have a fundamental understanding of the adversary's operational methods, constraints, and basic motives but that they experience, as much as possible, the planning/operational environment. However, many of the operational methods that might be used to carry out a plot are "reusable": for example, there is a limited number of ways to enter the country or obtain funds that would be "reused" by any number of terrorist scenarios that require entry into the country. Therefore, we propose developing computerized tools that will free teams up to concentrate on the essential themes of the scenarios, with the repertoire of operational details automatically drawn upon as needed.

In addition to the Red Team, this process requires that the actions required by the scenario be translated into signatures such as data entries or intelligence reports that could be matched to data base entries. A Black team consisting of intelligence and signal processing experts would perform this translation process.

The challenges for this concept are great and Sandia is making initial investments to judge the feasibility of the concept. Among these challenges are:

- Can we develop large scale war gaming, red teaming and modeling efforts to generate enough seed scenarios and fragments to give enough coverage to provide significant advantage to human analysts?
- Can we develop rich enough data structures and tools for capturing scenarios developed by humans so that the data is computer manipulatible?
- Can we develop approaches to "scoring" scenarios so that we can control the complexity of the searching in these large data warehouses?
- Can we develop tools to allow scenarios developed anywhere in our national security apparatus to be entered into this system?
- Can we develop tools to make this data warehouse useful to analysts?
- Can we develop ways to connect this data warehouse with real collected data to find possible evidence of real world events indicated by scenarios in the data warehouse?
- Can we successfully deal with the associated security issues and create the "need-to-know" access required for this type of database to be useful to multiple levels of users?
- Will this just create more databases that need to be searched thereby doubling the data mining tasks of today or will this help to focus data mining in a significant way?

Contacts:
John Whitley, jbwhitl@sandia.gov, 505-845-9763
Judy Moore, jhmoore@sandia.gov, 505-845-9415

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin
Company, for the United States Department of Energy's National Nuclear Security
Administration under contract DE-AC04-94AL85000.
SAND2003-4260P